APPLICATION FOR UNITED STATES LETTERS PATENT

of

Robert L. Faulk Jr.
608 Oakborough Avenue
Roseville, California 95747

for

DYNAMIC ACCESS CONTROL LISTS

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80527-2400

File No. 200313930-1

Certificate of Mailing Under 37 C.F.R. § 1.10

Express Mail Label No. ER394246255US Date of Deposit: April 8, 2004
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date indicated above and is addressed to: MS PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature

DYNAMIC ACCESS CONTROL LISTS

BACKGROUND OF THE INVENTION

[001] In an Ethernet local area network (LAN), computers or hosts are attached to the network and each host is uniquely identified by a physical address which is designated a media access control (MAC) address in an Ethernet network. The MAC address of each host is typically hardwired into an Ethernet network interface card in the host. The network interface card in each host transmits and receives Ethernet packets to communicate with the other hosts in the network. Each Ethernet packet includes an address segment including the MAC address of the host to receive the packet (destination MAC address) along with the MAC address of the host sending the packet (source MAC address), and further includes a data segment, as will be understood by those skilled in the art. The MAC address of each host is utilized by Ethernet switches in the network to receive and forward Ethernet packets between hosts. More specifically, a switch receives an Ethernet packet from a source host, examines the destination MAC address portion of the packet to determine where to forward the packet, and forwards the packet to the host corresponding to the destination MAC address.

[002] In many situations, an Ethernet network must communicate with hosts outside the network and in different types of networks. For example, a user of a host in an Ethernet network may want to access various Web sites and Web pages contained on the Internet. To communicate with other types of networks, the host utilizes the Internet Protocol (IP) which allows hosts in many different types of networks to communicate with each other through IP packets. Within the Ethernet network, each host must be assigned an IP address by a network administrator for the purpose of communicating with computers outside the network via the Internet Protocol. Devices known as routers operate to forward IP packets from one network to another utilizing the IP addresses contained in the IP packets being communicated.

[003] A router typically includes an access control list (ACL) to restrict or define the hosts with which a given host is allowed to communicate. For example, in an Ethernet network within a company, the hosts of employees may be restricted from

communicating with certain Web sites. In this way, access control lists are utilized as a tool for network security to define or control the hosts and other objects, such as files and directories, with which a given host can communicate. For example, IP packets from a particular IP network or a particular Web site may be restricted from being received by hosts in the Ethernet network. In this situation, the access control list on the router would contain a field indicating that packets from the IP address corresponding to this Web site are to be denied, meaning that any such packets received by the router will not be forward to the intended host in the Ethernet network. IP packets include source and destination IP addresses, with the source IP address corresponding to the IP address of the host that sent the packet and the destination IP address corresponding to the host that is to receive the packet.

[004] In an Ethernet network, there are two ways for a network administrator to assign IP addresses to hosts in the network. First, the network administrator can manually enter an IP address into a configuration file that is stored on each host. With large networks, this approach is typically not practical due to the amount of time it would take to configure all the hosts. As a result, the second approach that may be used is the configuration of a dynamic host configuration protocol (DHCP) server. The DHCP server operates to automatically assign IP addresses to hosts requesting an IP address instead of requiring the network administrator to manually assign such addresses. Typically, the DHCP server has a pool of available IP addresses that are assigned to requesting hosts as needed. When using a DHCP server to automatically assign IP addresses, the IP address for a given Ethernet host can change depending on the available IP addresses in the pool at the time the host requests the IP address. The use of a static ACL on a router to control access for a given Ethernet host does not work when a DHCP server is utilized since the IP address of the host is not static but changes over time. As a result, the static ACL having a set IP address for a given host does not allow the ACL to control access for that host when an IP address assigned to the host by the DHCP server is different than the IP address contained in the ACL.

[005] In an Ethernet network, a user must typically log onto a host in the network to gain access to the network and other host coupled to the network. This is typically done through a centralized authentication server which authenticates the credentials of a particular user. For example, in a Microsoft Windows environment a Windows NT Domain Login is utilized to authenticate the credentials of a user before allowing that user access to the network via his host. A domain defines a group of computers and devices on a network that are administered as a unit with common rules and procedures, and a user provides a Windows NT Domain Login in the form of a user name and password to gain access to or log into the network. Another example is the login procedure utilized where an IEEE 802.11 wireless device wants to communicate with an Ethernet network. In this situation, the wireless device communicates login information to an Ethernet switch that also functions as an access point for the device to access the network, and the switch, in turn, communicates with a remote access and dial-in user service (RADIUS) server to verify the credentials of the user.

[006] In some networks, there is no login procedure and user information is inferred directly from the MAC address of the host. Note that as used herein, the term host includes any type of electronic device that may be coupled to the network, such as a computer system, IP telephone, or personal digital assistant (PDA). For example, if a user "John Doe" has an IP telephone that begins sending Ethernet packets to the Ethernet network, then this IP telephone will be recognized using John Doe's Ethernet MAC address assigned to the telephone. A network administrator must configure the network in advance to define the MAC address for the IP telephone as a valid address within the network. Note that a user may log into the network on a number of different hosts and thus can have multiple MAC and IP addresses that will change as the user logs onto the network through different hosts. In many situations, access to resources within the network would ideally be restricted based upon user information regardless of the host through which the user is attempting to access the network.

[007] In a network that communicates through the IP protocol, hosts are identified not only by their IP address but also by a "domain name" that is utilized

instead of the IP address. As will be appreciated by those skilled in the art, a domain name such as "www.hp.com" may be registered with Internet domain name registration authorities to provide a plain English name that is easily remembered and recognized by users. Domain name system (DNS) servers contained in the Internet convert the domain name into a corresponding IP address which allows a host to communicate with a desired host corresponding to that IP address. There may be multiple IP addresses associated with a single domain name, and thus once again the use of a conventional ACL based upon a single IP address will not adequately restrict communication between a source host and destination host unless the ACL includes all such IP addresses. In the following description, the term "DNS name" will be used to refer to the domain name utilized by DNS servers and having an associated IP address, and the term "domain name" will be used to refer to groups of hosts in an Ethernet network that are administered as a unit such as a Windows NT domain name. Although the above examples are described with reference to an Ethernet network, the concepts of principles of the present invention may be applied to other types of networks, as will be appreciated by those skilled in the art.

[008] There is a need for access control lists that allows access of hosts in a computer network such as an Ethernet network to be restricted or controlled based upon user names, MAC addresses, domain names, and DNS names instead of merely IP address information.

SUMMARY OF THE INVENTION

[009] According to one aspect of the present invention, a method controls access of a user to a network including a plurality of hosts coupled together through a network switch. The method includes storing in the network switch an enhanced access control list containing data related to at least one of user names, DNS names, domain names, and physical addresses. A dynamic access control list is generated from the enhanced access control list, with the dynamic access control list containing a plurality of IP addresses that restrict access of the user to the network.

BRIEF DESCRIPTION OF THE DRAWINGS

[010] **FIG. 1** is a functional block diagram of an Ethernet network including an Ethernet switch that utilizes a dynamic access control list to restrict the access of computers in the network according to one embodiment of the present invention.

[011] **FIG. 2** is a functional flow diagram illustrating the process executed by the Ethernet switch of **FIG. 1** in generating a dynamic access control list according to one embodiment of the present invention.

[012] **FIG. 3** is more detailed functional block diagram of the Ethernet switch of **FIG. 1** according to one embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[013] **FIG. 1** is a functional block diagram of an Ethernet network ***100*** including an Ethernet switch ***102*** that utilizes a dynamic access control list ***104*** to restrict the access of users to hosts ***106a-n*** in the network according to one embodiment of the present invention. In operation, the switch ***102*** generates the dynamic access control list ***104*** containing IP addresses currently being utilized by various users of the network ***100***, and utilizes the dynamic access control list to restrict the access of such users to hosts ***106a-n*** in the network. In generating the dynamic access control list, the switch ***102*** utilizes an enhanced access control list ***108*** containing IP address, user name, DNS name, Windows domain name, and MAC address information for the users and hosts ***106a-n*** of the network ***100***. The switch ***102*** uses the information contained in the enhanced access control list ***108*** to determine current IP addresses for users accessing the network ***100*** and for hosts ***106a-n*** requesting such IP address, and then stores the determined IP addresses in the dynamic access control list ***104*** to control the access of users and hosts to the network based upon the IP addresses in the dynamic access control list, as will be explained in more detail below.

[014] In this way, the switch ***102*** allows user access to the network ***100*** to be controlled regardless of the host ***106a-n*** through which the user is accessing the

network and allows access to be controlled based upon IP address, user name, DNS name, Windows domain name, and/or MAC address information instead of merely static IP address information. Moreover, the switch ***102*** can be utilized in networks ***100*** containing a DHCP server (not shown) that dynamically allocates IP addresses to the hosts ***106a-n*** since the dynamic access control list ***104*** will contain the current IP address assigned to each host by the DHCP server.

[015] In the following description, certain details are set forth in conjunction with the described embodiments of the present invention to provide a sufficient understanding of the invention. One skilled in the art will appreciate, however, that the invention may be practiced without these particular details. Furthermore, one skilled in the art will appreciate that the example embodiments described below do not limit the scope of the present invention, and will also understand that various modifications, equivalents, and combinations of the disclosed embodiments and components of such embodiments are within the scope of the present invention. Embodiments including fewer than all the components of any of the respective described embodiments may also be within the scope of the present invention although not expressly described in detail below. Finally, the operation of well known components and/or processes has not been shown or described in detail below to avoid unnecessarily obscuring the present invention.

[016] In the network ***100***, the hosts ***106a-n*** are coupled to ports P1-PN, respectively, of the Ethernet switch ***102***, and the switch forwards Ethernet packets from a source host (a host sending a packet) to a destination host (a host to which the packet is directed). More specifically, the switch ***102*** examines the destination MAC address portion of each received Ethernet packet and forwards the packet to the host ***106a-n*** corresponding to the destination MAC address. This corresponds to the conventional operation of an Ethernet switch. In addition to the conventional operation of forwarding and receiving Ethernet packets, the switch ***102*** also determines whether each Ethernet packet is from a new host ***106a-n*** on the port P1-PN. If the source MAC address of the new host is not in an address table of the switch ***102***, or is in the address table on a different port, the switch will recognize the new source MAC address.

[017] The switch ***102*** also determines whether each Ethernet packet from a host ***106a-n*** is a "login packet." Login packets are sent by a host ***106a-n*** when a user is first attempting to access the network ***100*** through that host. Login packets convey the user name and password data for the user, and also includes the source MAC address of the host ***106a-n*** the user is utilizing to access the network. A login request will be directed to an authentication server, which is not expressly shown in **FIG. 1** but which corresponds to one of the hosts ***106a-n***. The switch ***102*** also detects the login acknowledge packets being returned from the authentication server for the originating host ***106a-n*** in response to the login request. The switch ***102*** determines whether the user has been granted access from the login acknowledge packets, and if the user has been granted access the switch ***102*** associates the user name with the MAC address of the host ***106a-n*** the user is utilizing. The switch ***102*** stores this association as an entry or record in a mapping state database ***110***, with the record containing the user name and the MAC address corresponding to the host ***106a-n*** the user is currently using to access the network ***100***.

[018] The switch ***102*** also detects all dynamic host configuration protocol (DHCP) packets sent by any of the hosts ***106a-n***. A host ***106a-n*** sends DHCP packets to a DHCP server, which although not shown in **FIG. 1**, would correspond to one of the hosts to thereby obtain an IP address when required, such as when the host is going to access the Internet. The DHCP packets will contain a source MAC address corresponding to the host ***106a-n*** that sent the DHCP packets and thus the host that is requesting the IP address. The switch ***102*** then monitors the return DHCP packets from the DHCP server sent in response to the DHCP packets, and from these return DHCP packets determines the IP address assigned to the host ***106a-n*** requesting the IP address. At this point, the switch knows the IP address assigned to a particular MAC address.

[019] Since prior to sending the DHCP packet the host ***106a-n*** being used by the user would have previously sent a login packet, the mapping state database ***110*** will at this point contain a record indicating a user name associated with the MAC address of the host ***106a-n*** that just requested the IP address. As a result,

the switch ***102*** at this point has determined an IP address associated with a particular MAC address which, in turn, is associated with a particular user. The enhanced access control list ***108*** also includes rules or access privileges for each user (*i.e.*, user name), and the switch ***102*** applies these rules to generate a corresponding entry or record in the dynamic access control list ***104*** for the user. The switch ***102*** thereafter applies the dynamic access control list ***104*** to control the access of the user to resources in the network ***100***, such as other hosts ***106a-n***, files, directories, Web sites, and so on.

[020] As previously mentioned, the enhanced access control list ***108*** may include DNS names. The switch ***102*** uses such DNS names to generate additional IP address records in the dynamic access control list ***104*** to limit user access to specific Web sites, for example, as will be explained in more detail below. Briefly, the switch ***102*** uses the DNS name in the enhanced access control list ***108*** to obtain an IP address corresponding to the DNS name, and then utilizes this IP address in the dynamic access control list ***104*** to restrict a users access to the IP address corresponding to this DNS name. The same is true of Windows domain names contained in the enhanced access control list ***108***, as will also be explained in more detail below.

[021] The switch ***102*** utilizes any IP addresses contained in the enhanced access control list ***108*** to generate corresponding entries in the dynamic access control list ***104***. Also note that the enhanced access control list need not include all of the indicated name and address information, but may include any subcombination of these information elements depending on the needs of the network ***100***. For example, the enhanced access control list ***108*** may include only IP address, MAC address, and user name information elements.

[022] **FIG. 2** is a functional flow diagram illustrating the process executed by the Ethernet switch ***102*** of **FIG. 1** in generating the dynamic access control list ***104*** according to one embodiment of the present invention. The dynamic access control list ***104***, enhanced dynamic access control list ***108***, and mapping state database ***110*** previously discussed with reference to **FIG. 1** are shown in **FIG. 2**. The overall process executed by the Ethernet switch ***102*** includes three

subprocesses: 1) a user name monitoring and conversion subprocess ***200***; 2) a DNS name monitoring and conversion subprocess ***202***; and 3) a DHCP monitoring and MAC conversion subprocess ***204***. These subprocesses operate in combination to apply the rules contained in the enhanced access control list ***108*** to generate the mapping state database ***110*** and dynamic access control list ***104***, as will now be described in more detail.

[023] In operation, the user name monitoring and conversion subprocess ***200*** converts user names into either MAC or IP addresses depending upon the manner in which a user is attempting to log into the network ***100***. When a user is attempting to log into the network ***100*** using a host ***106*** (**FIG. 1**) that communicates through the IEEE 802.1x standard, the host being utilized by the user will communicate login packets to the network ***100***. The IEEE 802.1x standard defines a group of communications protocols through which devices communicate with a local area network such as the network ***100***, as will be appreciated by those skilled in the art. The login packets will include a user name and password along with a MAC address associated with the host ***106*** being utilized by the user. The subprocess ***200*** monitors a login reply packet sent by the network ***100*** to the host ***106*** being utilized by the user in response to the login packet to determine whether the user has been granted access to the network. When the subprocess ***200*** determines the user has been granted access, the subprocess associates the user name from the login packets with the MAC address of the host ***106*** being utilized by the user and stores this information as a record in the mapping state database ***110***. In this way, the subprocess ***200*** maps user names to MAC addresses when a user is accessing the network ***100*** with a host ***106*** that communicates via the IEEE 802.1x protocol. If the MAC address is new and thus not currently stored in the mapping state database ***110***, the subprocess ***200*** also supplies the MAC address to the DHCP monitoring and MAC conversion subprocess ***204*** for determination of the IP address associated with the new MAC address, as will be described in more detail below.

[024] The user name monitoring and conversion subprocess ***200*** also operates to determine an IP address associated with a particular user name when a user is

attempting to access the network ***100*** using a Windows host ***106***. More specifically, when hosts ***106*** in the network ***100*** run the Windows operating system, a Windows domain controller, which corresponds to one of the hosts, is responsible for granting or denying access of a user to the network. To access the network ***100***, a host ***106*** being utilized by the user and the host functioning as the domain controller communicate server message block (SMB) login packets. Each SMB login packet includes a user name associated with the user and a computer name associated with the host ***106*** being utilized by the user. In response to the SMB login packet, the domain controller will supply a SMB login reply packet to the host ***106*** being utilized by the user, and this packet will include an IP address assigned to the host being utilized by the user. This reply packet will also contain information either granting or denying the user access to the network ***100***. If the user is granted access to the network ***100***, the subprocess ***200*** will associate the IP address contained in the SMB login reply packet with the user name and apply the rules from the enhanced access control list ***108*** for this user name to generate corresponding records in the dynamic access control list ***104***. Note that if the presently determined IP address associated with the user name is different from an IP address for that user name previously stored in the dynamic access control list ***104***, both the new and the previous IP address(es) are stored for the user. This allows one Enhanced ACL entry to be created for the user, which is applied to all of the hosts ***106*** that the user has logged into, simultaneously.

[025] It should be noted that the user name data contained in a SMB login packet is encrypted, and thus the subprocess ***200*** must have access to the corresponding encryption key in order to decrypt this data and obtain the user name. If the encryption key is not available, then the subprocess ***200*** could associate the computer name contained in the SMB login packet, which is not encrypted, with the IP address contained in the SMB login reply packet and store this information in the mapping state database ***110***.

[026] The DNS name monitoring and conversion subprocess ***202*** operates to determine DNS names corresponding to IP addresses contained in packets being communicated over the network ***100***. More specifically, the subprocess ***202***

detects all Ethernet packets being communicated through the switch ***102*** (**FIG. 1**) having a source IP address which does not yet exist in the mapping state database ***110***. As will be appreciated by those skilled in the art, all packets being communicated over the network ***100*** are Ethernet packets when the network is an Ethernet network. In this situation, however, IP packets are contained within these Ethernet packets when the IP protocol is being utilized, with this nesting of packets of a particular protocol within packets of another protocol typically being referred to as a protocol stack, as will be understood by those skilled in the art. Accordingly, the subprocess ***202*** can detect all unknown source IP addresses contained in packets being communicated through the switch ***102***.

[027] When the subprocess ***202*** detects an unknown source IP address, the subprocess generates a reverse DNS lookup query containing the source IP address, and sends this query to a DNS server. In response to the reverse DNS lookup query, the DNS server determines a DNS name corresponding to the source IP address and returns this DNS name to the switch ***102***. The subprocess ***202*** then stores the DNS name associated with this particular source IP address in the mapping state database ***110*** and applies the rules of the enhanced access control list ***108*** to develop a corresponding record for the dynamic access control list ***104***. It should be noted that there may be multiple records in the enhanced access control list ***108*** for a given DNS name. As a result, the subprocess ***202*** may develop a number of corresponding records for the dynamic access control list ***104***.

[028] Over time new IP addresses may be assigned to particular DNS names and for proper operation of the switch ***102*** the subprocess ***202*** must detect any such changes and properly update the dynamic access control list ***104***. This may be accomplished by the subprocess ***202*** occasionally sending reverse DNS lookup queries to the DNS server for each DNS name in the mapping state database ***110*** and detecting any changes. Another approach is to have the DNS server configured to automatically inform the subprocess ***202*** when a new IP address is assigned to a given DNS name, enabling the subprocess to update the dynamic access control list ***104*** as required.

[029] The third subprocess executed by the switch ***102*** is the DHCP monitoring and MAC conversion subprocess ***204***, which converts MAC addresses into corresponding IP addresses. The subprocess ***204*** monitors DHCP return packets from a DHCP server, which corresponds to one of the hosts ***106*** (**FIG. 1**), and from these return packets determines the IP address assigned by the DHCP server to a given MAC address. Recall, in response to a request from a given host ***106*** the DHCP server assigns an IP addresses to that host from a pool of available IP addresses. Thus, the subprocess ***204*** need merely determine the assigned IP address contained in the return packet for the destination MAC address of the packet. The subprocess ***204*** stores a record of the IP address assigned to the MAC address in the mapping state database ***110*** and applies the rules of the enhanced access control list ***108*** to generate a corresponding record in the dynamic access control list ***104***.

[030] If a prior IP address for the MAC address is already stored in the mapping state database ***110***, this record is deleted and updated with the new IP address and the dynamic access control list ***104*** updated accordingly. When MAC addresses are statically assigned to the hosts ***106***, the subprocess ***204*** monitors address resolution protocol (ARP) packets, where the ARP is a network protocol used to convert IP addresses into physical addresses such as Ethernet addresses, as will be understood by those skilled in the art. Each ARP packet will include the IP and MAC address of the host ***106*** sending the packet, and thus the subprocess ***204*** detects such packets to determine the IP address associated with each MAC address and updates the mapping state database ***110*** and dynamic access control list ***104*** accordingly. Alternatively, packets with new source IP addresses can be given to the CPU as was described in the DNS monitoring process. Through this method, the the IP and MAC address of the host ***106*** sending the packet is identified , and thus the subprocess ***204*** detects such packets to determine the IP address associated with each MAC address and updates the mapping state database ***110*** and dynamic access control list ***104*** accordingly

[031] During operation of the switch ***102***, it is possible that different user names or MAC addresses may attempt to be mapped to the same IP address, which

should not be allowed and would represent an error condition. For example, assume a given host ***106*** has a MAC address "123456-123456" and has been statically assigned an IP address of 192.168.0.1. Also assume there is a rule in the enhanced access control list ***108*** for the MAC address 123456-123456. If there is a separate rule contained in the enhanced access control list ***108*** for a user "John Doe" and John Doe logs into the network using the host ***106*** corresponding to the MAC address 123456-123456 then the user name and John Doe and the MAC address 123456-123456 will mapped to the same IP address. This may not be a problem, but if John Doe has different access privileges to resources in the network ***100*** then does the MAC address 123456-123456 then a conflict and thus an error condition exists. For example, the access privileges of John Doe may be more restrictive than those of the MAC address 123456-123456, and in this situation and John Doe should not be provided access to the network ***100*** with the less restrictive access privileges associated with the MAC address.

[032] Such a conflict may be resolved by generating a "deny" record in the dynamic access control list ***104*** for this IP address so that no packets are communicated to or from the host ***106*** corresponding to the IP address. Alternatively, the rule first encountered in the enhanced access control list ***108*** could be applied, such that if the rule for MAC address 123456-123456 appears in the enhanced access control list prior to the rule for user name and John Doe, the rule for the MAC address is utilized. In this way, as long as levels of access privileges are taken into account when generating the enhanced access control list ***108*** such conflicts can be resolved without denying all packets to and from the corresponding host ***106***. Furthermore, either of the above approaches could also include sending an error notification to a system administrator to notify him or her of the conflict.

[033] Over time, the IP address configuration changes will occur on the network ***100***. For example, the administrator may reconfigure the DHCP server to allocate a different pool of IP addresses, or the network administrator may reconfigure hosts ***106*** with new static IP addresses. The DHCP server may allocate a different address to a given user. These IP address configuration

changes could appear as an error condition. To prevent this, stale data must be purged from the mapping state database ***110***, and the associated entries in the Dynamic ACL ***104*** should be deleted. Mapping state database ***110*** entries populated via DHCP monitoring are deleted after a DHCP lease time expires, or when DHCP packets are received from the DCHP server which give a previously allocated IP address to a new user. Mapping state database ***110*** entries populated via ARP monitoring or IP source address change monitoring are deleted after an administratively configured time. One day is a good default value for this timeout.

[034] **FIG. 3** is more detailed functional block diagram of the Ethernet switch ***102*** of **FIG. 1** according to one embodiment of the present invention. The Ethernet switch ***102*** includes a switch forwarding engine ***300*** that examines Ethernet packets received on one of a plurality of ports P1-PN from a host (not shown) coupled to each port and forwards each received Ethernet packet to the proper host through the corresponding port. A processor ***302*** in the switch ***102*** programs the switch forwarding engine ***300*** to execute a desired set of rules to provide selected Ethernet packets received by the forwarding engine to the processor. The set of rules ensures that the processor ***302*** receives all packets necessary for the proper generation of the dynamic access control list ***104*** (**FIG. 2**). In the embodiment of **FIG. 3**, the switch forwarding engine ***300*** provides all IEEE 802.1x login packets, Windows domain login packets, packets having unknown source IP addresses, and DHCP packets as previously described to the processor ***302*** to enable the processor execute the process previously described with reference to **FIG. 2**.

[035] The switch ***102*** further includes a direct memory access (DMA) controller ***304*** that transfers the packets selected by the switch forwarding engine ***300*** to a packet memory ***306***. The selected packets are stored in the packet memory ***306*** for processing by the processor ***302***. Also stored in either the packet memory ***306*** or memory in the processor ***302*** is the enhanced access control list ***108*** (**FIG. 2**) along with required programming instructions for execution by the processor to control the overall operation of the switch ***102***. To store a selected packet from the switch forwarding engine ***300***, the processor ***302*** programs required registers in the

DMA controller ***304***. The switch forwarding engine ***300*** then supplies the packet to the DMA controller ***304*** which, in turn, stores the packet in the packet memory ***306***. The processor ***302*** accesses the stored packets in the packet memory ***306*** along with the stored enhanced access control list ***108*** (**FIG. 2**) to generate the dynamic access control list ***104*** (**FIG. 2**). After the processor ***302*** processes a given packet stored in the packet memory ***306***, the packet may need to be provided to the intended destination host ***106***. To forward a packet stored in the packet memory ***306*** to the intended destination host ***106***, the processor ***302*** addresses the packet memory to access the desired packet and programs required registers in the DMA controller ***304***. In response to being programmed, the DMA controller ***304*** reads the accessed packets from the packet memory ***306*** and supplies these packets to the switch forwarding engine ***300*** which, in turn, forwards the packets to the required destination host ***106***.

[036] One skilled in the art will understand that even though various embodiments and advantages of the present invention have been set forth in the foregoing description, the above disclosure is illustrative only, and changes may be made in detail, and yet remain within the broad principles of the invention. For example, many of the components described above may be implemented using either digital or analog circuitry, or a combination of both, and also, where appropriate, may be realized through software executing on suitable processing circuitry. One skilled in the art will also appreciate that the functions performed by the dynamic access control list ***104***, enhanced access control list ***108***, mapping state database ***110***, subprocesses ***200-204***, and components ***300-306*** may be combined to be performed by fewer elements or divided out and performed by more elements, depending upon the specific application of the switch ***102*** and possibly other design considerations. Moreover, although the above embodiments have been described for the Ethernet network ***100***, the concepts of principles of the present invention may be applied to other types of networks, as will be appreciated by those skilled in the art. Therefore, the present invention is to be limited only by the appended claims.